EXHIBIT O

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

19MAG2296.

In the Matter of Warrant for All Content and Other Information Associated with (1) the iCloud account associated with the user ID and/or email address [redacted]; (2) the iCloud account associated with the user ID and/or email address [redacted] and (3) the iCloud account associated with the user ID and/or email address [redacted], Maintained at Premises Controlled by Apple, Inc., USAO Reference No. 2016R00246.

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for Search Warrants for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

DIANA CHAU, Postal Inspector, United States Postal Inspection Service, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Postal Inspector with the U.S. Postal Inspection Service (the "USPIS" or "Investigating Agency"). As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. During my tenure with the USPIS, I have participated in the investigations of numerous frauds, and have conducted physical and electronic surveillance, the execution of search warrants, debriefings of informants, and reviews of taped conversations. Through my training, education,

and experience, I have become familiar with the manner in which securities frauds and insider trading offenses are perpetrated.

B. The Provider, the Subject Accounts, and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with:

a. The iCloud account associated with the user ID and/or email address [redacted], maintained and controlled by Apple, Inc. ("Apple," or the "Provider"), with offices in Cupertino, California ("SUBJECT ACCOUNT-1");

b. The iCloud account associated with the user ID and/or email address [redacted], maintained and controlled by the Provider ("SUBJECT ACCOUNT-2,"); and

c. The iCloud account associated with the user ID and/or email address [redacted], maintained and controlled by the Provider ("SUBJECT ACCOUNT-3," and collectively with SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-2, the "SUBJECT ACCOUNTS");

Based on my review of records obtained from Apple pursuant to a grand jury subpoena, I know that SUBJECT ACCOUNT-1 is subscribed in the name of Pete Petit ("PETIT") and is an active account that was created on or about November 20, 2010; that SUBJECT ACCOUNT-2 is subscribed in the name of William Taylor ("TAYLOR") and is an active account that was created on or about May 25, 2012; and that SUBJECT ACCOUNT-3 is subscribed in the name of [redacted] and together with PETIT and TAYLOR, the "TARGET SUBJECTS") and is an active account that was created on or about October 27, 2011.

3. As detailed below, there is probable cause to believe (i) that SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-2 contain evidence, fruits, and instrumentalities of an accounting fraud scheme perpetrated by the PETIT, TAYLOR, and others in connection with their employer, MiMedx Group, Inc. ("MiMedx," or the "Company"), in violation of Title 18, United States Code, Sections 1343 (wire fraud), 1348 (securities fraud), 1350 (improper certification of financial

reports by corporate officers); Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Sections 240.10b-5 (securities fraud) (collectively, the "Accounting Fraud Offenses"); and aiding and abetting and conspiring to commit the Accounting Fraud Offenses, in violation of Title 18, United States Code, Section 2 (aiding and abetting), 371 (conspiracy) and 1349 (conspiracy); and (ii) that SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-3 contain evidence, fruits, and instrumentalities of an insider trading scheme perpetrated by PETIT, [redacted] and others in the publicly traded shares of MiMedx, in violation of Title 18, United States Code, Sections 1343 (wire fraud), 1348 (securities fraud); Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Sections 240.10b-5 (securities fraud) (collectively, the "Insider Trading Offenses"); and aiding and abetting and conspiring to commit the Insider Trading Offenses, in violation of Title 18, United States Code, Section 2 (aiding and abetting), 371 (conspiracy) and 1349 (conspiracy). The Accounting Fraud and Insider Trading Offenses taken together are referred to herein as the "SUBJECT OFFENSES."

4. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers and employees of the United States Securities and Exchange Commission ("SEC"), as well as my training and experience concerning the use of electronically stored information in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents or other evidence and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

5. I have learned the following about the Provider:

a. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple also provides a variety of services that can be accessed from Apple devices or, in certain cases, from other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include, in certain instances, email, instant messages services, and file storage:

i. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

ii. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls. iMessage is oftentimes used in place of, or in addition to, standard Short Message Service text message communications.

iii. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

iv. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to

synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

v. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

vi. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location. Certain of this information is stored on the phone and may be backed up to the iCloud. Find My iPhone similarly allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

vii. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

b. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

c. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

d. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

e. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs"

for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

f. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

g. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS")

messages, voicemail messages, call history, browser history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

D. Jurisdiction and Authority to Issue Warrants

6. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

7. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

8. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause Regarding the Subject Offenses

Relevant Individuals and Entities

9. Based on my review of publicly available information, my review of records produced by MiMedx in response to a subpoena from the SEC, and my conversations with personnel and

representatives of MiMedx and other companies that conducted business with MiMedx, I have learned the following, in substance and in part:

a. MiMedx Group, Inc. is a biopharmaceutical company headquartered in Marietta, Georgia, that develops and markets regenerative and therapeutic biologics using human placental tissue allografts, colloquially referred to as wound care products or tissues. At all relevant times, MiMedx was a publicly traded company, listed on the NASDAQ exchange. MiMedx distributed its wound care products to end users directly as well as through independent distributors.

b. PETIT was MiMedx's chief executive officer ("CEO") between approximately 2008 and 2018. PETIT resigned from his position at MiMedx on or about June 30, 2018, in lieu of being terminated by MiMedx's board of directors.

c. TAYLOR was MiMedx's chief operating officer ("COO") between approximately 2009 and 2018. In his role as COO, TAYLOR reported directly to, and worked closely with, PETIT. TAYLOR resigned from his position at MiMedx on or about June 30, 2018, in lieu of being terminated by MiMedx's board of directors.

A. Probable Cause Concerning the Accounting Fraud Offenses

10. As described in greater detail below, there is probable cause to believe that from at least 2012 through 2017, MiMedx, through its senior management and directors, routinely and knowingly filed public financial reports with the SEC that contained false and inflated earnings information, with the intent to deceive the investing public. Specifically, during the relevant period, MiMedx improperly recognized revenue from the purported sale of its products in violation of generally accepted accounting principles ("GAAP") and relevant regulations and guidance

promulgated by the SEC. MiMedx then falsely reported this inflated revenue to the investing public, including through its financial filings with the SEC.

11. On or about February 20, 2018, MiMedx issued a press release and filed a Form 8K with the SEC, announcing that the filing of the company's reports of financial results for fourth quarter 2017 and fiscal year 2017 would be delayed and that the company's audit committee had begun "an internal investigation into current and prior-period matters relating to allegations regarding certain sales and distribution practices at the Company." To date, MiMedx has not filed its financial results for fourth quarter 2017 or fiscal year 2017.

12. On or about June 6, 2018, MiMedx announced that its previously issued financial statements for the years 2012 through 2016 and for the first three quarters of 2017 needed to be restated and should no longer be relied upon. Pursuant to applicable federal law, PETIT had certified each of MiMedx's annual SEC filings (i.e., Form 10-K) during that period. In announcing the need to restate those filings, MiMedx explained that "the determination of the need to restate was based on investigation results to date which have primarily been focused on the accounting treatment afforded to such sales and distribution practices for two distributors for which certain implicit arrangements modified the explicit terms of the contracts, impacting revenue recognition during specified periods."

13. AvKare, Inc, is a Tennessee-based medical supply company, which, based on conversations with representatives of MiMedx's audit committee, I understand was one of the two distributors referenced in MiMedx's June 6, 2018 announcement. In or about April 2012, MiMedx and AvKare entered into a purported Product Distribution Agreement, under which, in sum and substance, AvKare became the exclusive distributor for "EpiFix," a MiMedx wound healing product, in the Veterans Affairs ("VA") hospital system. AvKare, unlike MiMedx at the time, was

on the Federal Supply Schedule, which allowed it to sell products into the VA system. As discussed below and in practice, however, MiMedx sales representatives, and not AvKare employees, were the individuals who distributed MiMedx products in the VA system.

Relevant Accounting Principles

14. Generally accepted accounting principles (GAAP) refer to a common set of accounting principles, standards and procedures that companies must follow (represent that they follow) when preparing and filing financial statements. GAAP is meant to ensure a minimum level of methodological consistency across the financial statements of different companies, which makes it easier for investors to analyze and extract useful information and compare GAAP metrics across different companies. For publicly traded companies, the SEC also promulgates accounting rules and guidance that companies must follow when filing their financial reports.

15. Under GAAP and SEC guidance, a company that engages in the sale of products through a distributor may recognize revenue upon transfer of the product to a distributor if, among other things, collectability (i.e., receiving payment) is reasonably assured. When the distributor has a right of return (i.e., the ability to return the product without having to pay for it), revenue cannot be properly recognized unless all of the following criteria are met: (1) the seller's price to the buyer is fixed or determinable at the date of sale; (2) the buyer's obligation to pay the seller is not contingent on the resale of the product; (3) the buyer's obligation to pay the seller is not excused in the event that the product is damaged or lost; (4) the buyer has economic substance separate from the seller; (5) the seller does not have significant obligations for future performance to directly bring about the resale of the product by the buyer; and (6) the amount of future returns can be reasonably estimated. *See, e.g.*, Accounting Standards Codification, Subtopic 605-15-25-1.

MiMedx's Relationship with AvKare and Inappropriate Revenue Recognition

16. Based upon interviews with MiMedx and AvKare personnel, review of company documents, and conversations with representatives of MiMedx, investigators have learned the following facts about MiMedx's relationship with AvKare during the period from 2012 to 2017:

a. During the relevant period, distribution through AvKare was the primary means by which MiMedx sold its products to VA hospitals. These sales, in turn, accounted for a significant part of MiMedx's revenue.

b. Although AvKare nominally acted as a distributor of MiMedx's products within the VA system, in practice, AvKare employees played little role in marketing or distributing MiMedx products. Rather, MiMedx maintained what the company called a "federal sales force," whose members were responsible for interacting with VA employees, monitoring the stock of MiMedx product on the shelves at VA hospitals, and keeping track of when tissue was implanted in patients.

c. When MiMedx's personnel determined that a particular VA facility was in need of tissue, they notified MiMedx's sales department, which then shipped the product directly to the VA facility. Although AvKare was notified of the shipment, no AvKare employees were physically involved in handling the product. During the relevant period, MiMedx treated such shipments as sales to AvKare and recognized revenue at the time of shipment. In practice, however, AvKare was under no obligation to pay MiMedx for the tissue until the VA purchased it from AvKare, generally at the time of implantation. Moreover, because AvKare had a limited sales force of its own, MiMedx employees were responsible for promoting MiMedx products to VA doctors and facilities.

d. Moreover, despite the fact that MiMedx recognized revenue for tissue at the time of shipment to the VA, during the relevant period, MiMedx routinely issued AvKare credits for lost or damaged tissue, even after it had been shipped to the VA. As TAYLOR explained to an AvKare principal in an email dated March 8, 2013:

> Contractually, AvKare owns the inventory once received (under the new amendment, once shipped), but practically speaking, MiMedx will work with AvKare if any issues arise with the inventory. Some recent examples highlight this. Over the past few months, several grafts have been dropped or otherwise lost and MiMedx replaced them at no cost to AvKare. Because MiMedx is directing the placements in the 120+ VAs we service, we obviously are very involved with the inventory management and will not leave you with any losses!

e. Nor was it the case that AvKare's obligation to pay MiMedx for shipped tissue existed independent of AvKare's ability to resell the product to the VA. Indeed, beginning in April 2015, the product distribution agreement between AvKare and MiMedx explicitly provided that in the event the relationship were to terminate, MiMedx would "repurchase any remaining inventory of Products from AvKare at the price paid by AvKare for such Products."

f. From conversations with representatives of MiMedx, I have learned that the company's decision to re-state its earnings was prompted, in part, by the conclusion that, based on the information above, MiMedx's practice of recognizing revenue at the time tissue was shipped was inconsistent with GAAP and SEC guidance.

17. In addition, based on my review of documents produced by MiMedx, I have learned that MiMedx recognized revenue upon shipment from sales to certain distributors other than AvKare in which cases MiMedx also apparently excused payment until resale and/or agreed to post-sale obligations. For example, on or about December 21, 2015, TAYLOR wrote in connection with the sale of approximately $2.5 million of products to a Saudi-based medical distributor known as First Medical that "[i]n the event that the tender is delayed, or for some

unlikely event it does not occur, MiMedx will give First Medical additional extended payment terms if requested, and will assist First Medical in selling the product or another option would be to repurchase the product." Based on my training and experience and my participation in this investigation, I understand that TAYLOR was stating that MiMedx could repurchase the product from First Medical; that First Medical's obligation to pay was contingent on resale; and/or that MiMedx would undertake obligations for future performance to bring about resale.

18. Based on my review of MiMedx records, I have learned that MiMedx nevertheless recognized this entire sales amount (approximately $2.5 million) as revenue in the fourth quarter of 2015. After that time, First Medical struggled to make payments and did not pay for the product until in or about 2017. On or about March 25, 2016, PETIT wrote to a number of MiMedx executives about First Medical, noting that he was "not optimistic about [F]irst [M]edical. We might squeeze something out of them just to show progress." From speaking with representatives of MiMedx, I understand that First Medical is the second distributor referenced in the June 6, 2018 Mimedx press release referring to "two distributors for which certain implicit arrangements modified the explicit terms of the contracts, impacting revenue recognition during specified periods."

19. As set forth above, in or about June 2018, PETIT and TAYLOR resigned from MiMedx. Following PETIT and TAYLOR's resignations, they submitted through counsel a memorandum laying out various justifications for their conduct. In the memo, PETIT and TAYLOR argue, among other things, (a) that they were generally uninformed about the GAAP principles governing revenue recognition, and (b) that they relied in good faith on accounting professionals, the audit committee, outside auditors, and lawyers. These assertions however are not consistent with documents and other evidence that I have received and reviewed from MiMedx.

Furthermore, based on my review of documents and communications exchanged between MiMedx senior management and its auditors and audit committee, and my conversations with members of MiMedx's auditors and audit committee, I do not believe that Mimedx's lawyers, auditors, and/or the audit committee were informed of certain facts concerning the MiMedx-AvKare relationship including, among other things, (a) that the extent to which MiMedx salespeople were responsible for selling the tissue to the VA and ensuring that the VA paid AvKare, and (b) the fact that MiMedx tracked what the VA paid AvKare to anticipate when and how much AvKare would pay MiMedx.

B. Probable Cause Concerning the Insider Trading Offenses

20. I further submit that there is probable cause to believe that in or about January and February of 2018, PETIT, [redacted] and others engaged in insider trading by converting material non-public information ("MNPI") that PETIT had obtained by virtue of his employment at MiMedx to his own use for personal gain. In particular, [redacted] avoided at least approximately $2 million in losses by selling MiMedx stock from in and around late January to late February 2018, shortly before the Company announced a delay in the release of its 10-K filing, which caused a 36 percent decrease in the stock price.

MiMedx's Share Price Decreases as a Result of Delayed Financial Filings

21. As set forth above, based on my review of MiMedx documents and from speaking with Company personnel and representatives, I have learned that in or about August 2017, MiMedx engaged Ernst and Young ("EY") as an external auditor. From speaking with representatives of EY, I have learned that over the course of January and February 2018, EY conveyed to MiMedx management that in light of the amount of work necessary to investigate MiMedx's prior revenue recognition practices, MiMedx would not be able to file its annual 10-K on time, *i.e.*, by March of

2018. Based on my training and experience, I am aware that a company's inability to file a timely 10-K usually causes a company's stock price to decline.

22. In particular, from speaking with representatives of MiMedx and EY, and my review of documents produced by MiMedx and obtained from FINRA, I have learned of the following developments that occurred in early 2018:

a. On or about January 23, 2018, MiMedx managers, including PETIT and TAYLOR, had a meeting with EY that was scheduled with the subject "Audit Meeitng" [sic]. During the meeting, EY discussed concerns about MiMedx's accounting practices concerning AvKare.

b. On or about January 25 and 26, 2018, MiMedx managers, including PETIT and TAYLOR, participated in an email exchange with the subject "E&Y." In an email on January 26, MiMedx's CFO noted that "I am sure we all realize that this extra review and focus by EY puts the timely filing of our financial statements in jeopardy. We need to move quickly to avoid any delays." In response, PETIT wrote that he was "now concerned"; that he wanted EY to speak with the CFO and others directly; and that "[t]his has reached the point where I want to be involved in almost every conversation."

c. On or about February 6, 2018, EY met with MiMedx's audit committee and told them that the Company needed an independent investigation concerning its sales and distribution practices before MiMedx's 2017 financial statements could be filed. At the meeting, EY raised the possibility that in light of these circumstances, MiMedx might not meet its regulatory filing deadlines. Over the next few days, MiMedx engaged a law firm—King & Spalding LLP—and an accounting firm—KPMG—to conduct the independent investigation.

d. On or about February 16, 2018, EY met with MiMedx management again concerning the investigation of MiMedx's sales and distribution practices. During this meeting, EY advised that MiMedx would not be able to file its 2017 10-K by March.

e. On or about February 20, 2018, MiMedx issued the aforementioned press release concerning the delay. Following the issuance of the press release, MiMedx's stock dropped approximately 36 percent from a share price of $15.38 to $9.90.

[redacted] *Avoided Significant Losses in MiMedx Stock*

23. From reviewing documents that I obtained from the Financial Industry Regulatory Authority ("FINRA") and the SEC, I have learned that [redacted] have at least two trading accounts at Fidelity Brokerage Services ("Fidelity"). I have also learned that between January 25 and February 15, 2018, [redacted] sold over 300,000 shares of MiMedx. Based on these timely sales, [redacted] avoided over $2 million in losses. For example, between January 25 and 29 – within days of MiMedx's CFO's January 26, 2018 email alerting PETIT of the "jeopardy" of delayed financial statements – [redacted] sold over 189,000 shares of MiMedx.[1]

24. In response to questions from FINRA that were submitted to the Company following this period, PETIT asserted through the Company in a submission to FINRA on or about June 13, 2018 that he was not aware of any circumstances under which [redacted] would have obtained knowledge of information concerning the Company's February 20 press release. PETIT further asserted that he "had no contact" with [redacted] from February 6 through February 16, 2018. Based on my review of documents provided by MiMedx, however, I have learned that on or about

[1] On or about February 13, 2018, [redacted] invested in certain short term put options that would be valuable if MiMedx stock increased. The value of these options was less than $50. Based on my training and experience, I submit that the investment in a small amount of options, while reducing a substantial equity position, is a potential attempt to conceal illegal trading based on MNPI.

February 7, 2018, PETIT and [redacted] communicated via iMessage. Based upon information shared by MiMedx's outside counsel, which oversaw a review of MiMedx's review of PETIT's electronic devices, I have learned that this iMessage (or messages) are no longer available because they appear to have been deleted by PETIT, along with dozens of other iMessages that had been stored on PETIT's company-issued phone, at some time before that phone was returned to the Company in or about August 2018.[2]

C. Probable Cause Regarding the Subject Accounts

Use of SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-2 in Connection with the Accounting Fraud Offenses

25. I submit that there is probable cause to believe that SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-2 will contain evidence of the Accounting Fraud offenses. Based on my review of documents obtained from MiMedx, I have learned that PETIT frequently communicated about MiMedx's relationship with AvKare and other distributors, increasing sales at the end of quarters, and MiMedx's communications with auditors, among other things, through various email addresses, including his MiMedx-issued email address. For example, on or about December 11, 2015, a Company sales executive sent an email to PETIT, TAYLOR, and others stating that "[e]ach quarter we credit AvKare a significant amount of revenue . . . Taking these credits makes it significantly harder to reach our quarter end goals." PETIT responded approximately 20 minutes later, complaining that "[t]hese problems are caused by one thing ..... LACK OF MANAGEMENT." Based on my training and experience, I believe that this email is discussing,

[2] In or about January 2012, PETIT was also the subject of SEC enforcement action into alleged insider trading by PETIT and an associate. The associate settled with the SEC without any acknowledgement of wrongdoing, and the SEC dropped its case against PETIT. In or about January 2016, TD Ameritrade terminated its relationship with [redacted] on suspicion that [redacted] were involved in insider trading with respect to the shares of MiMedx.

among other things, the fact that MiMedx often gave credit to AvKare for tissues when AvKare was not paid by the VA.

26. Based on my review of records obtained from Apple, I have learned that SUBJECT ACCOUNT-1 was created in or about 2010 and, between 2010 and 2018 had approximately ten iPads and five iPhones registered to it. SUBJECT ACCOUNT-1 was also often accessed using iPads and iPhones, including for services such as "backup," which I understand to mean the transfer of files from the iPad or iPhone to iCloud for secondary storage.[3] As part of my investigation, I have also reviewed dozens of videos that were taken of meetings of MiMedx senior management in PETIT's boardroom at the Company's headquarters.[4] For example, in a meeting in or about August 3, 2017, PETIT and others were discussing a draft of a press release that made mention of the role that MiMedx salespeople played at the VA, *i.e.*, MiMedx's efforts to bring about resale of products sold to AvKare. In the video, MiMedx's CFO recommends taking this description out, noting that "There is one section in here that gets into very specifics on what AvKare is doing and what we're doing, I think you're inviting the SEC to come after us." Throughout this meeting, and others that I have reviewed, PETIT is present in the conference room with his iPad constantly receiving and sending electronic communications, as seen by the audible notification of incoming messages that can be heard regularly throughout. In other videos that I have observed, PETIT can be seen and heard using voice dictation to compose outgoing messages from his iPad.

---

[3] Access logs provided by Apple only go back a number of days. Thus, the access logs that I have reviewed show constant access by an iPad and iPhone to SUBJECT ACCOUNT-1, but only going back to December 2018. Based on that activity, however, I submit that PETIT has probably been accessing SUBJECT ACCOUNT-1 by iPad and iPhone in a similar, constant fashion since he began actively using the account in 2010.

[4] The recordings were made when a recording device that PETIT had installed in his conference room was inadvertently left on continuously for a number of months.

27. From speaking with representatives of MiMedx, I have learned that PETIT was able to access at least four separate email accounts – including his MiMedx-issued email account, from which the December 11, 2015 email cited in paragraph 25 above was sent – from at least one iPad that PETIT used at MiMedx. Accordingly, and because PETIT was regularly using iPads to communicate with MiMedx personnel and others over email about the Accounting Fraud Offenses, I submit that SUBJECT ACCOUNT-1 will contain relevant evidence of the Accounting Fraud Offenses.

28. I have also seen iMessages involving SUBJECT ACCOUNT-2 that relate to MiMedx's relationships with certain distributors. For example, in paragraph 17-18 above, I described a transaction involving revenue recognition with First Medical. Following the transaction, in or about January 20, 2016, a MiMedx employee prepared an audit confirmation for First Medical to sign confirming to MiMedx's then-external auditor, Cherry Bekaert, that First Medical's balance was due and owing. The audit confirmation asked First Medical to "indicate any special sales or payments terms related to this balance." On or about February 12, 2016, TAYLOR exchanged iMessages from an email account associated with SUBJECT ACCOUNT-2 with a MiMedx employee about ensuring that MiMedx audit confirmations, including First Medical's, got signed so that Cherry Bekaert could complete the audit for 2015. During that conversation, TAYLOR asked the other employee to see if First Medical "can send a draft of the signed letter to me prior to him sending to the auditors." TAYLOR then discussed getting an audit confirmation from another distributor to whom MiMedx had also extended flexible payment terms, and instructed that the audit confirmation should have "[n]o extra commentary. Just sign and send." Based on my training and experience, I understand TAYLOR to be expressing a concern that these distributors would disclose additional information (such as payment terms) in the audit

confirmation, which would potentially raise concerns about the propriety of MiMedx's recognizing revenue upon shipment of product to First Medical.

29. Following the exchange of these iMessages, First Medical returned a signed audit confirmation to Cherry Bekaert on or about February 15, 2016 that contained no mention of the payment terms described in TAYLOR's email quoted earlier in paragraph 17. Based on my training and experience, I understand that iMessages, like the ones described above, are sent and stored through iCloud accounts' messaging capabilities. Accordingly, I submit that there is probable cause to believe that SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-2 will contain communications related to the involvement of PETIT, TAYLOR, and/or others in the Accounting Fraud Offenses.

Use of SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-3 in Connection with the Insider Trading Offenses

30. As described in paragraph 24 above, I have also observed that PETIT corresponded with [redacted] via iMessage during the period in which MiMedx was initiating its internal investigation and when PETIT conveyed to FINRA that he had not communicated with [redacted]. Based on documents that I have obtained from Apple and others, I have observed that the phone number used by PETIT in that exchange is associated with at least one device that was associated with SUBJECT ACCOUNT-1, and that the number used by [redacted] in that exchange is associated with SUBJECT ACCOUNT-3. Both of those accounts were also associated with a number of iPhones which, based on my training and experience, I understand can save such text messages and back them up to an iCloud account. Accordingly, I submit that there is probable cause to believe that SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-3 will contain communications related to the involvement of PETIT, [redacted] and/or others in the Insider Trading Offenses.

31. In addition to the foregoing, based on my training and experience, I know that email records oftentimes contain evidence of the crime of securities fraud, including lies to auditors and insider trading, conspiring to commit securities fraud, and aiding and abetting securities fraud. In this case, I submit that based on the foregoing there is probable cause to believe that the TARGET SUBJECTS used the SUBJECT ACCOUNTS to communicate about all means and manner of business at MiMedx including about the relationship between MiMedx and AvKare, MiMedx's relationship with other distributors, increasing sales at the end of quarters, MiMedx's communications with auditors, MiMedx's internal investigation, and communications related to the Company's stock. Accordingly, there is probable cause to believe that the SUBJECT ACCOUNTS are likely to contain additional emails that would include evidence of the SUBJECT OFFENSES.

32. Similarly, based on my training and experience, I know that iMessages, MMS, SMS, and other text message formats are frequently used by corporate executives and others to communicate about business matters. For example, as indicated above, TAYLOR used text messages as a way to communicate about obtaining audit confirmation from MiMedx distributors all in an attempt to prevent the Accounting Fraud Offenses from being discovered by MiMedx's auditors. In addition, text messages may contain evidence regarding a user's state of mind, including consciousness of guilt. Accordingly, there is probable cause to believe that the SUBJECT ACCOUNTS are likely to contain text messages that would include the same or similar categories of evidence described above.

33. Additionally, based on my training and experience, I know that browser histories often provide valuable insight into the mindset of individuals who are suspected of securities fraud and other offenses. In this case, browser history information recovered from the SUBJECT

ACCOUNTS would provide valuable insight into information regarding the users' state of mind, including potential consciousness of guilt and their awareness of the relevant laws and regulations related to revenue recognition, insider trading, and other aspects of the SUBJECT OFFENSES.

34. The requested Warrant and Order will be limited to (i) with respect to the Accounting Fraud Offenses, items sent, received, or created between January 1, 2012 and the present, inclusive, which is the period for which MiMedx has withdrawn (or not issued) financial statements due to a review of "sales and distribution practices"; and (ii) with respect to the Insider Trading Offenses, items sent, received, or created from August 2017 through August 2018, encompassing the time-period from which MiMedx engaged EY through the period when PETIT returned his MiMedx-issued phone to the Company, that contained the deleted iMessages referenced earlier.

Evidence, Fruit, and Instrumentalities

35. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the SUBJECT ACCOUNTS will contain evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, as more fully described in Section II of Attachment A to the proposed warrant.

36. In particular, I believe that SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-2 are likely to contain the following information:

- Evidence of the users of the accounts communicating regarding the Accounting Fraud Offenses, including improper revenue recognition practices and related sales practices at MiMedx, including, but not limited to, communications relating to the timing, quantity, nature and price of any purchase of MiMedx products by distributors/customers, the timing and terms of any payments to MiMedx by the distributors/customers, returns and credits offered to distributors/customers, and the involvement of MiMedx personnel in effectuating resales by MiMedx's distributor/customers;

- Evidence of the users of the accounts communicating regarding the provision of information to auditors, regulators, investigators, or any other party tasked with analyzing MiMedx's sales and revenue recognition practices;

- Evidence of the users of the accounts communicating regarding earnings and revenue targets or analyst projections;

- Evidence of state of mind, including but not limited to, consciousness of guilt and awareness of the propriety of revenue recognition practices at MiMedx or awareness of, or attempts to influence, any audits or investigations regarding MiMedx's revenue recognition or sales and distribution practices; and

- Evidence of the geographic location of users of the accounts, as well as the computer or device used to access the accounts, which may in turn lead to additional evidence.

37. Furthermore, I believe that SUBJECT ACCOUNT-1 and SUBJECT ACCOUNT-3 are likely to contain the following information:

- Evidence of the user of the accounts communicating regarding the Insider Trading Offenses, including but not limited to, communications relating to the sharing of information about the status of audits and/or investigations into MiMedx in 2018, the timing of MiMedx's SEC filings in 2018, the status or prospects for any MiMedx press release that was considered or issued by MiMedx, and any expected movements in the stock price of MiMedx;

- Evidence of the user of the accounts communicating regarding any trading, acquiring, selling, or otherwise transacting in the publicly traded shares of MiMedx;

- Evidence of state of mind, including but not limited to, awareness of the status of audits and/or investigations into MiMedx in 2018, the timing of MiMedx's SEC filings in 2018, the status or prospects for any MiMedx press release that was considered or issued by MiMedx, and any expected movements in the stock price of MiMedx; consciousness of guilt and awareness of, or attempts to hide, any insider trading activity; and

- Evidence of the geographic location of user of accounts, as well as the computer or device used to access the accounts, which may in turn lead to additional evidence.

III. Review of the Information Obtained Pursuant to the Warrants

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the

status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the SUBJECT OFFENSES as specified in Section III of Attachment A to the proposed warrant.

39. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, including but not limited to undertaking a cursory inspection of all emails and communications within the SUBJECT ACCOUNTS. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

40. The existence and scope of this ongoing criminal investigation is not publicly known.[5] As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that TARGET SUBJECTS and/or other targets of the investigation are known to use computers and electronic communications in furtherance of their activity, they could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

41. Accordingly, there is reason to believe that, were the Provider to notify the subscribers or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

42. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

---

[5] Although newspapers and other media sources have reported generally that MiMedx is under investigation by regulators, I believe that many of the specific facts and circumstances outlined in this Affidavit, including the TARGET SUBJECTS' efforts to mislead auditors and allegations that PETIT engaging in insider trading are not publicly known.

V.Conclusion

43. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

DIANA CHAU
Postal Inspector
United States Postal Inspection Service

MAR 0 7 2019

Sworn to before me this
____ day of March, 2019

S/Debra Freeman

HONORABLE DEBRA FREEMAN
United States Magistrate Judge
Southern District of New York

3.7.2019